Threat Awareness Portfolio (TAP)

Science and Technology Directorate

Office of Plans, Programs, and Requirements

Joseph Kielman
Director, Threat Awareness Portfolio
joseph.kielman@dhs.gov
202-254-5787

Homeland Security

Threat Awareness Definition

Mission Statement

Develop, test, and deliver – in collaboration with intelligence, law enforcement, and homeland security community agencies – tools and methodologies for assessing terrorist threats and understanding terrorism.

Strategic Objectives

- Develop computationally based tools and methodologies for assessing information about and creating, applying, and disseminating knowledge on terrorist threats and activities
- Determine the motives and intents of and identify terrorists by understanding the socio-political, cultural, economic, and behavioral aspects of terrorism and developing reliable biometric indicators
- Assess terrorist capabilities for developing and deploying threat agents

Homeland Security

Portfolio Customer Base

- **DHS analysts and operational personnel (OI&A, ICE, CBP) –** Providing technologies and techniques for threat assessment
- **S&T technical staff –** Informing decisions on science and technology development
- **Intelligence and Law Enforcement Community technical and analytical staff –** Collaborating on tool development and evaluation
- **Government, academic, and commercial research community –** Leading research in specialized areas

Homeland Security

Portfolio Strategies

- **Research and development through broad intramural and commercial programs and selective joint sponsorship of intergovernmental activities**
- **Establishment of nation-wide capabilities in specialized science and technology areas critical to understanding threat**
- **Development and refinement of methodologies usable for assessing capabilities as well as motives and intents**
- **Testbed activities to evaluate new science and technology available from government, industry, and academia and to validate DHS and other homeland security community requirements**
- **Pilots for operational systems**

Homeland Security

TAP Span of Interest (Influence)

Premises:

risk = f (threat, vulnerability, consequence)

threat = f (*capability*, motive & intent)

Programs:

Capability and Threat Assessment

Motivation and Intent Analysis

Knowledge Management Technologies

Homeland Security

TAP Program Areas

- All-WMD Capability Assessment and Nuclear Forensics and Attribution Program - Assessing capabilities of foreign and domestic terrorist groups to develop and deploy WMD threat agents and determining the source(s) of radiological materials

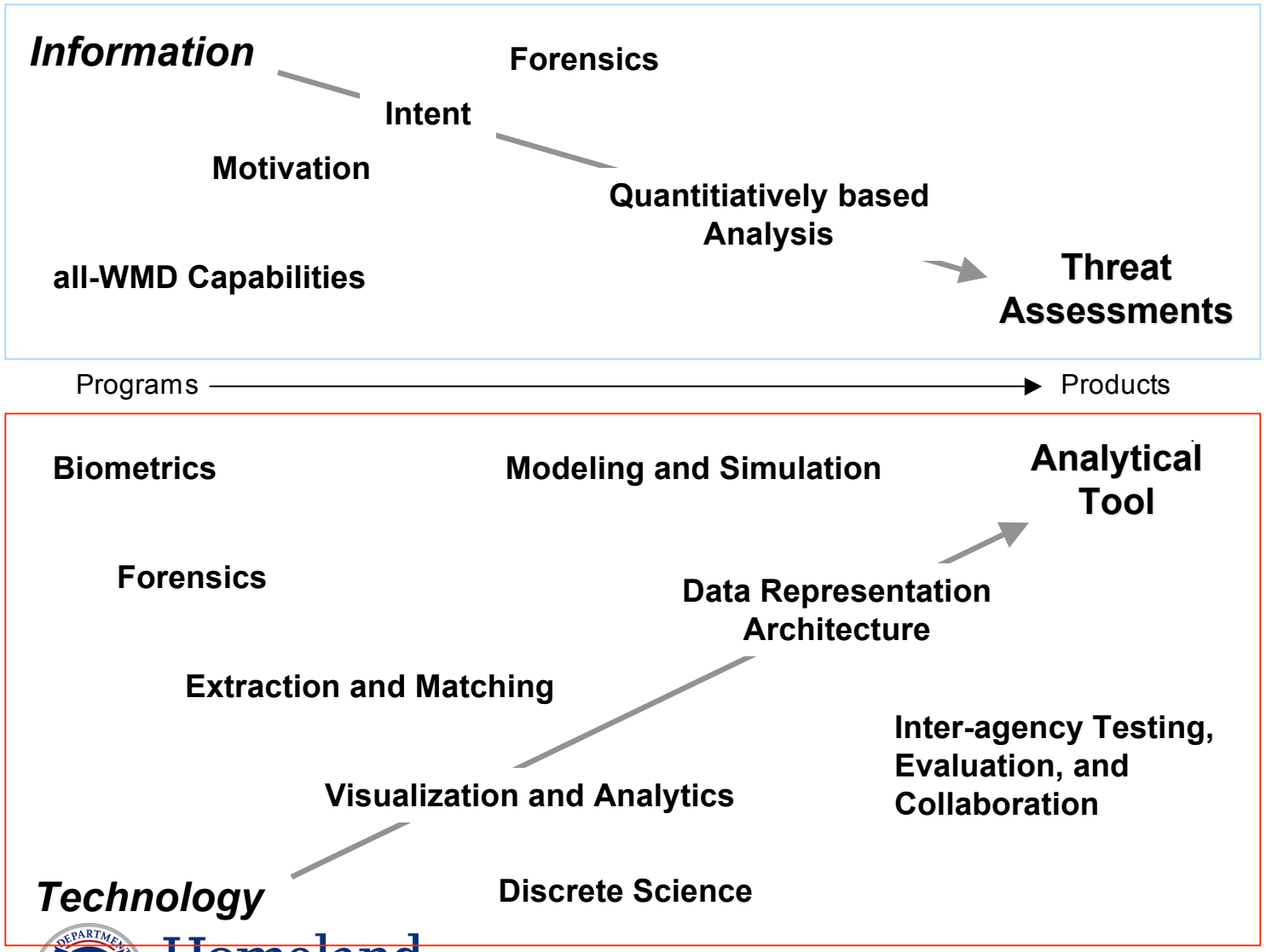
- Socio-political, Cultural, and Behavioral Factors - Understanding the motivations and intents of terrorists to develop predictive and prescriptive models that enable anticipation, preparation, and prevention
- Biometrics including Deception Detection - Technologies and techniques for verifying individual identity and identifying terrorists

- Data Science and Data Representation - Computing architecture for collecting, analyzing, and synthesizing massive amounts of threat information from multiple, distributed, and disparate data sources
- Visualization and Analytics - Techniques for visualizing, relating, and synthesizing information of multiple data types and from multiple sources
- Discrete Sciences and Modeling and Simulation - Advanced computing algorithms and hardware architectures for modeling, simulating, and managing threat data in real time and with high resolution

- Interagency Test and Evaluation - An interagency-supported facility for testing, evaluating, prototyping, and piloting knowledge management technologies for national-level threat assessment capabilities

Homeland Security

What Is TAP?



EITS

BorderSafe

Cargo

Actionable Knowledge

TVIS

RTAS

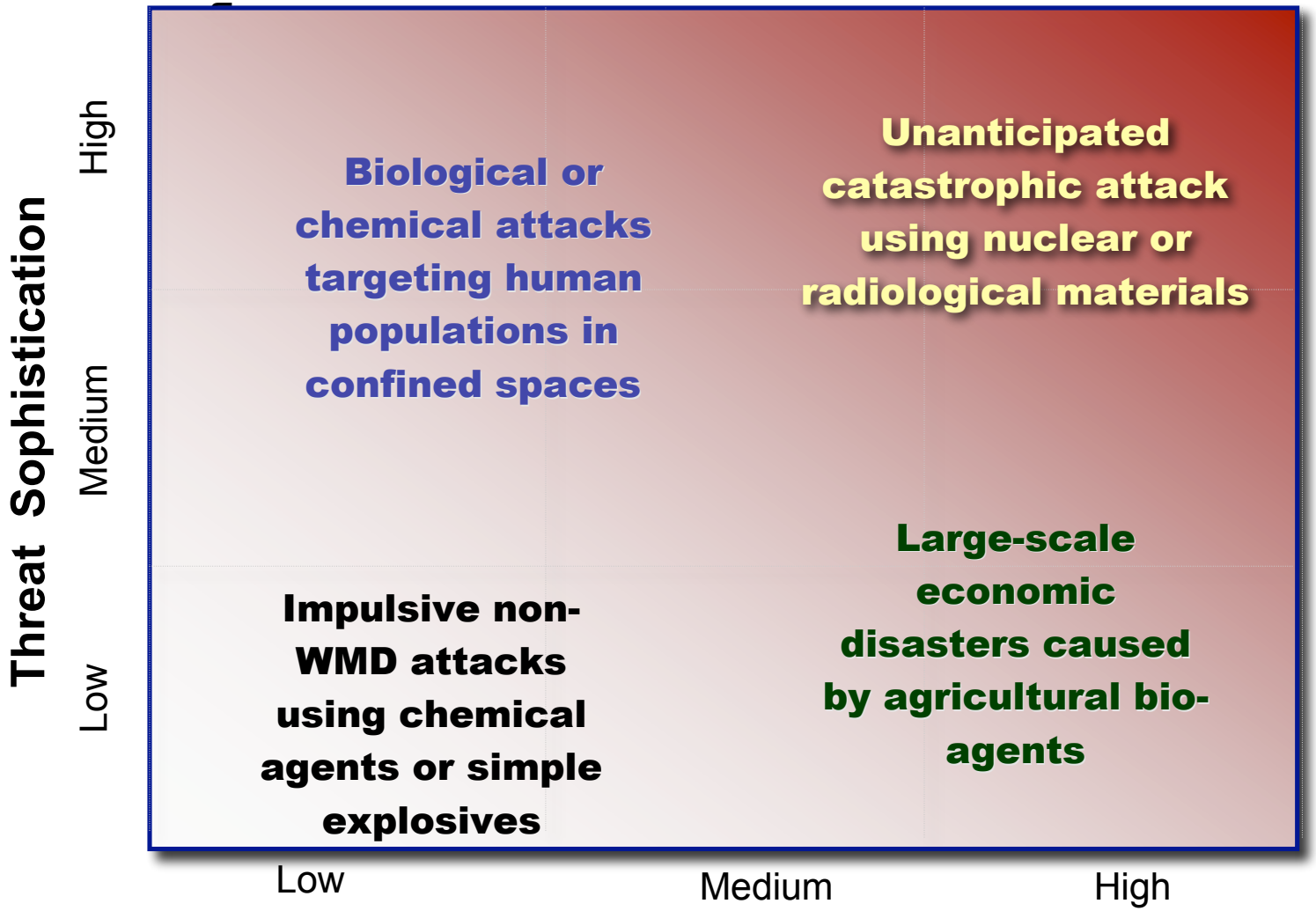
(all) or BKC

NTC

MAST

Homeland Security

Threat assessment techniques help analysts find actionable information to uncover planned attacks



Homeland Security

TAP research enables the creation of actionable information

- How credible is the reporting source (credibility)?
- Who is potentially threatening us (individual/group)?
- What are their stated motivations and observed threatening actions (doctrine and actions/tactics)?
- Where are they now (location)?
- Where might they attack us (target)?
- How might they attack us (weapon)?
- When might they attack us (urgency)?
- What's the possible outcome of an attack (consequence), and how does it change if the target is soft or security fails (vulnerability)?

By asking the right questions, DHS identifies the risk factors.

Homeland Security

CATPAW Products

Subjects

- Terrorist group baselines:
  - *locations, ideology, tactics*
- Terrorist group WMD capabilities
- Terrorist targets
- Terrorist networks
- Cross-cutting terrorist WMD issues
- Terrorist threats

Product Types

- Strategic analysis reports
- Targeted tactical analysis
- Reachback
- Support to analytical tool development
- Development/maintenance of web-based analytic compilation
- Structured databases

Homeland Security

Motivation and Intent

Definition of Problem Space

Motivational factors

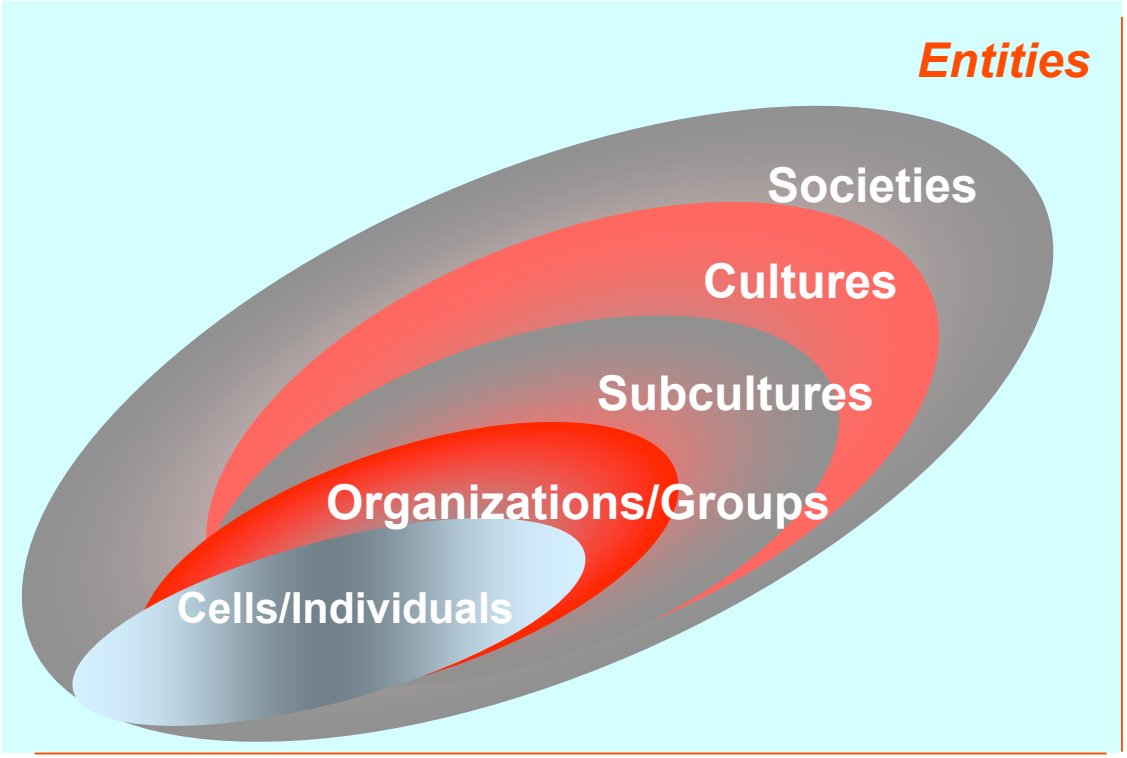
Unsatisfied needs

Ideologically antithetical to US

Desire negative impact on US - no resources

Preparing to act, have resources

Ready to act, have resources



Homeland Security

Requirements for Behavior Modeling and Simulation

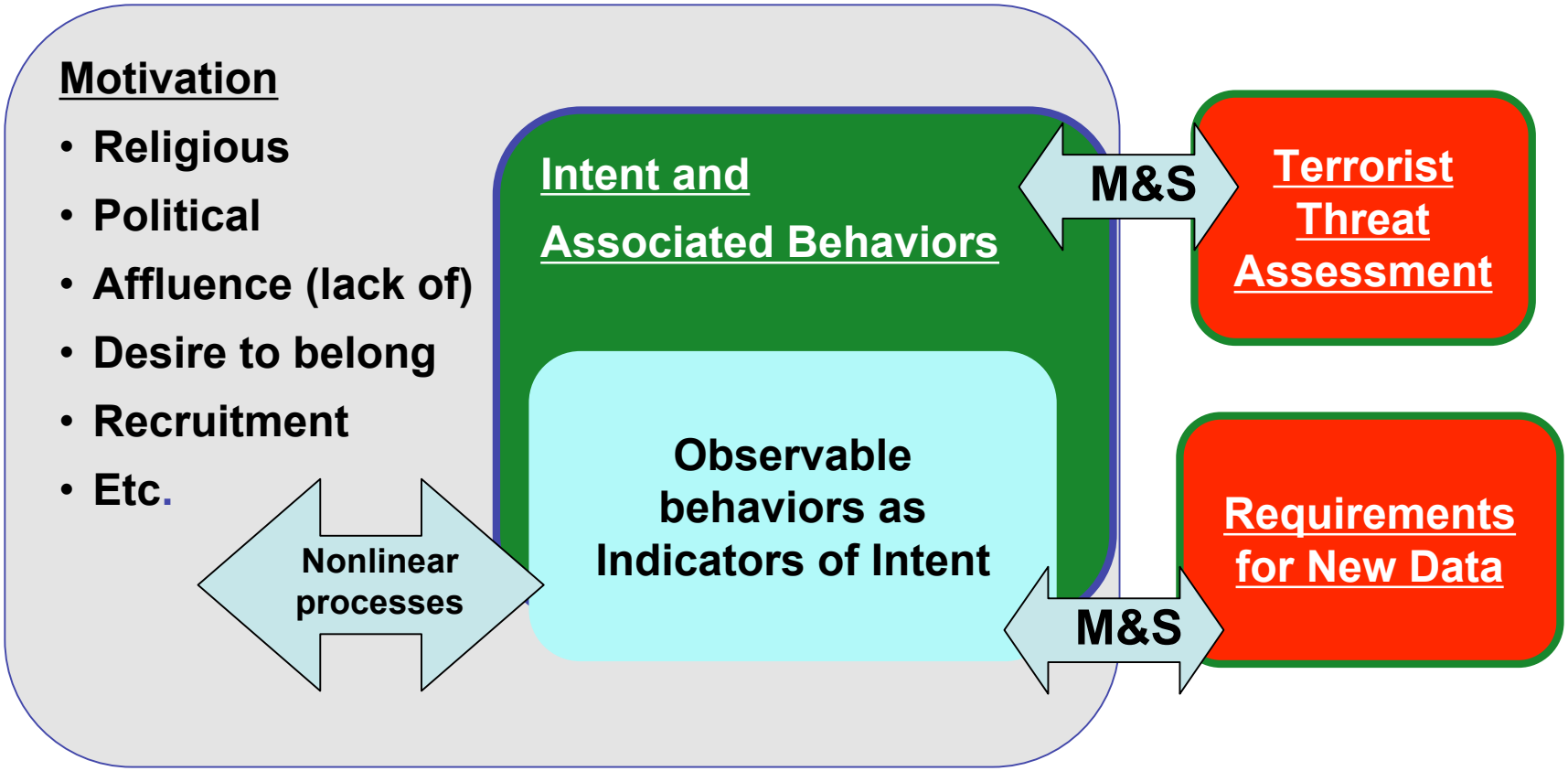
- *Value transference*
- *Ideological determinants*
- *Context for group and individual decision-making*

- *Emergence of leaders, followers*
- *Development of cells, swarms*
- *Dynamic network infrastructures*
- *Decision making processes*
- *Innovation, adaptation, and evolution*
- *Competition, collaboration, alienation among and within groups*
- *Identity formation and bond strengths*

- *Psychologically plausible cognitive decision-making models*
- *Micro-behaviors as intent indicators*

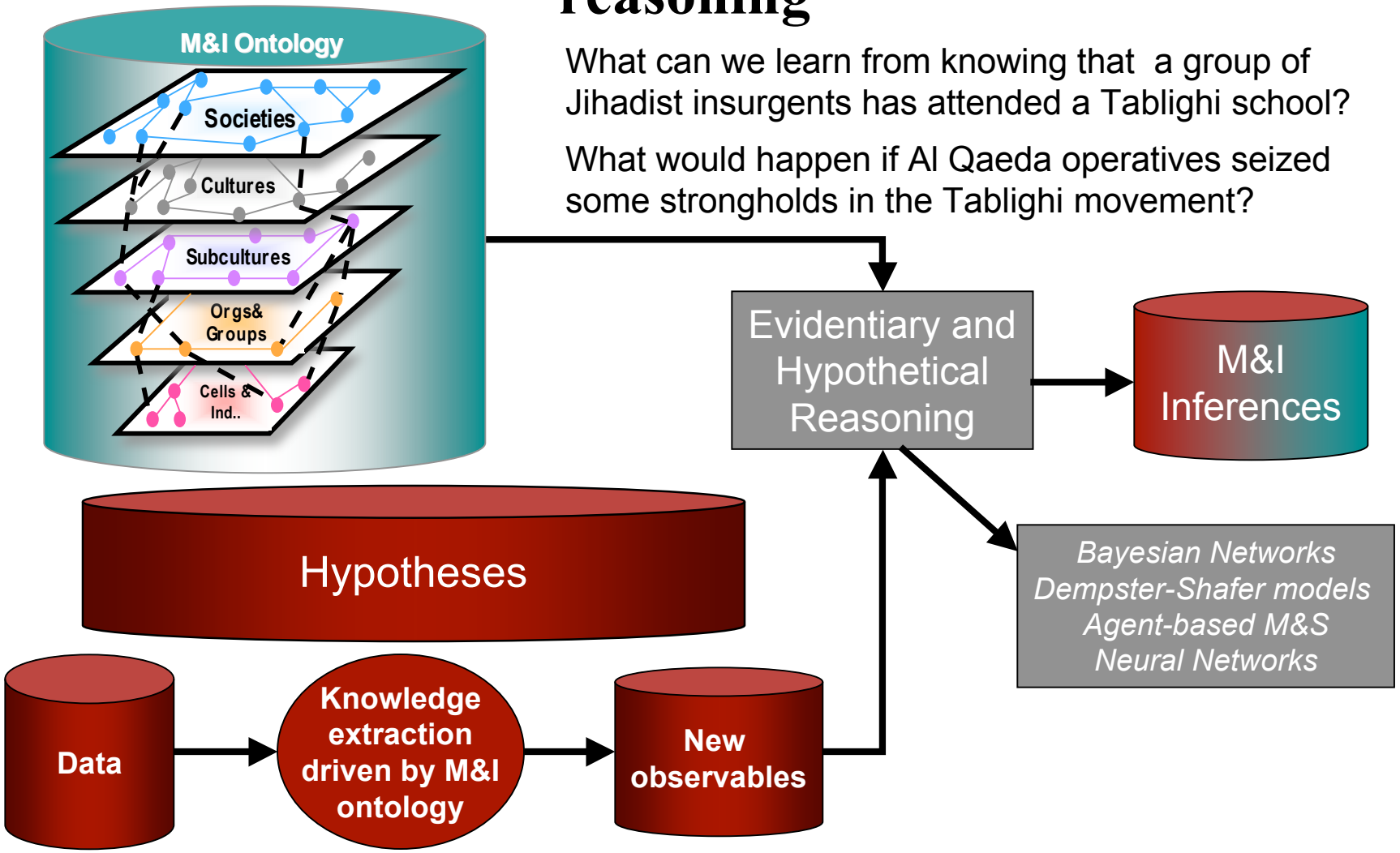
Homeland Security

How can we understand motivation and intent to better assess threats?



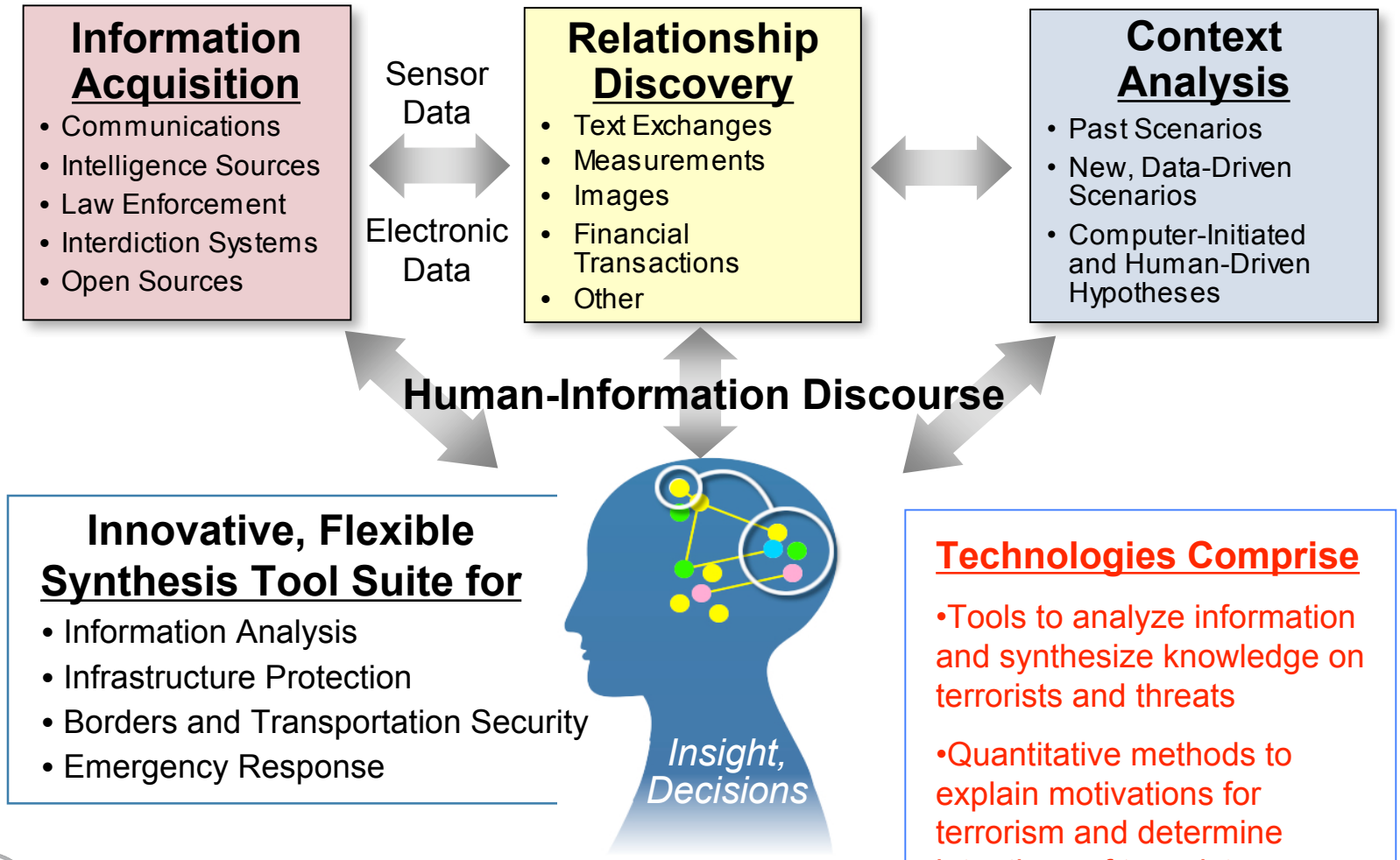
Homeland Security

Models based on ontologically driven probabilistic reasoning



Homeland Security

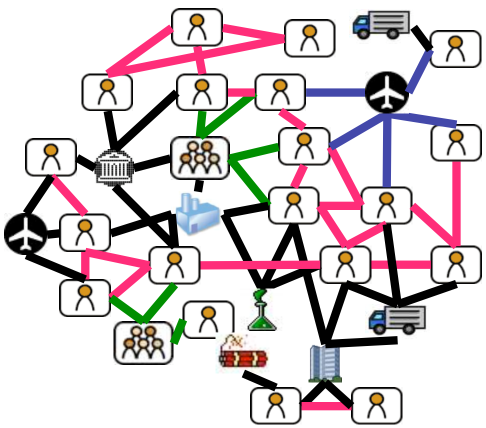
TAP technology helps to amplify user's ability to process information and assess real or potential threats



Homeland Security

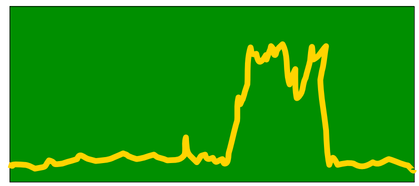
Current technical approaches rely on traditional threat detection technologies

Extract linked data



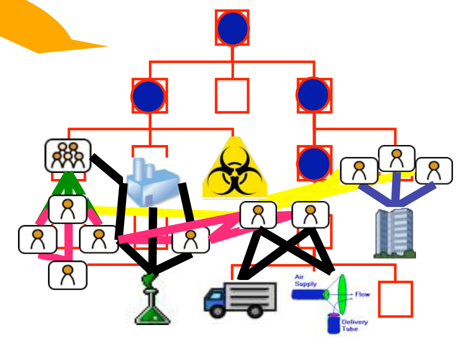
- Sample data to assemble multi-graph
- Use group detection to focus attention

Statistical Anomaly Detection



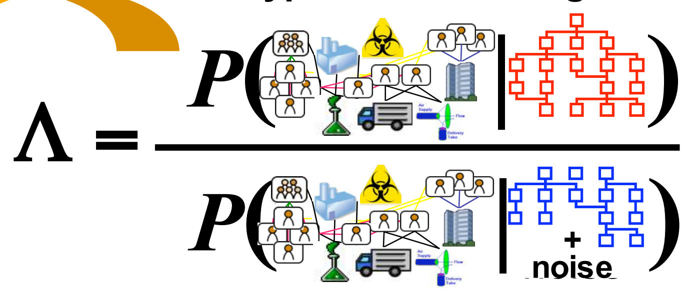
- Detect graphical statistical anomalies to identify potential threat networks
- Use as starting points for pattern matching searches

Pattern Matching



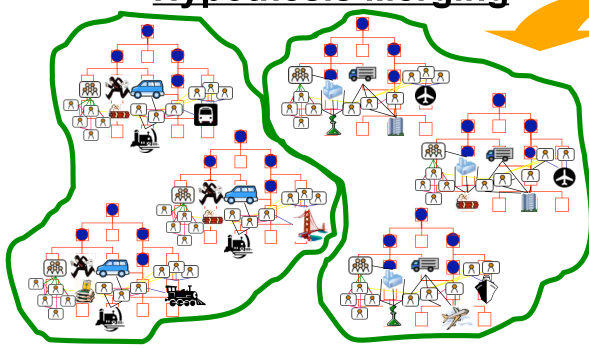
- Graph matching to find subtask signatures
- Connect related signatures to infer organized activities

Hypothesis Scoring



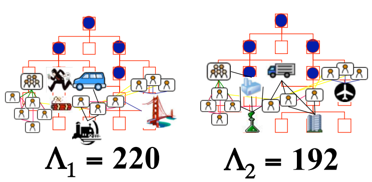
- Compute likelihood ratio for each hypothesis
- Filter and rank hypotheses

Hypothesis Merging



- Cluster and merge like hypotheses

Output to Analyst



Homeland Security

Information processing occurs on multiple levels

Process Area	Technology Recommendation	Technology Description
Connect the Dots	Information Aggregation Data integration	Software or hardware integration of multiple sources of information using different methods, and incorporating either structured or unstructured data. Collaboration of data sources, The making of connections between otherwise meaningless bits of information is at the core of (transnational) threat analysis.
Automated Content Management and Distribution	Ontological data processing Information Extraction	An Ontology "provides a vocabulary for representing and communicating knowledge about some topic". Ontological data processing provides the vocabulary and concept descriptions that allow for discussing the relationships between different data agents. Single Query supporting multiple source data mining across multiple security levels.
Advanced Analytics	Evidence Extraction and Link Discovery	Automatically extract relationships between people, organizations, places, and things. Techniques to extract entities from unstructured text and relations and patterns associated with terrorist activity.
	Pattern Analysis Information Visualization Concepts	Ways of visualizing information other than through text, lists, structured prose, and tables. Automation and cognitive aids to understand complex situations faster and more comprehensively. Delivered in different formats depending on intended use.
Information Assurance	Privacy Protection Software User Authentication	Effective privacy protection would allow for the relationships of agents to be preserved while protecting the unique identity of any specific agent. Select revelation, self-reporting data, immutable audits, privacy compliance. Single sign-on functionality with strong identity management across multiple security levels.

Homeland Security

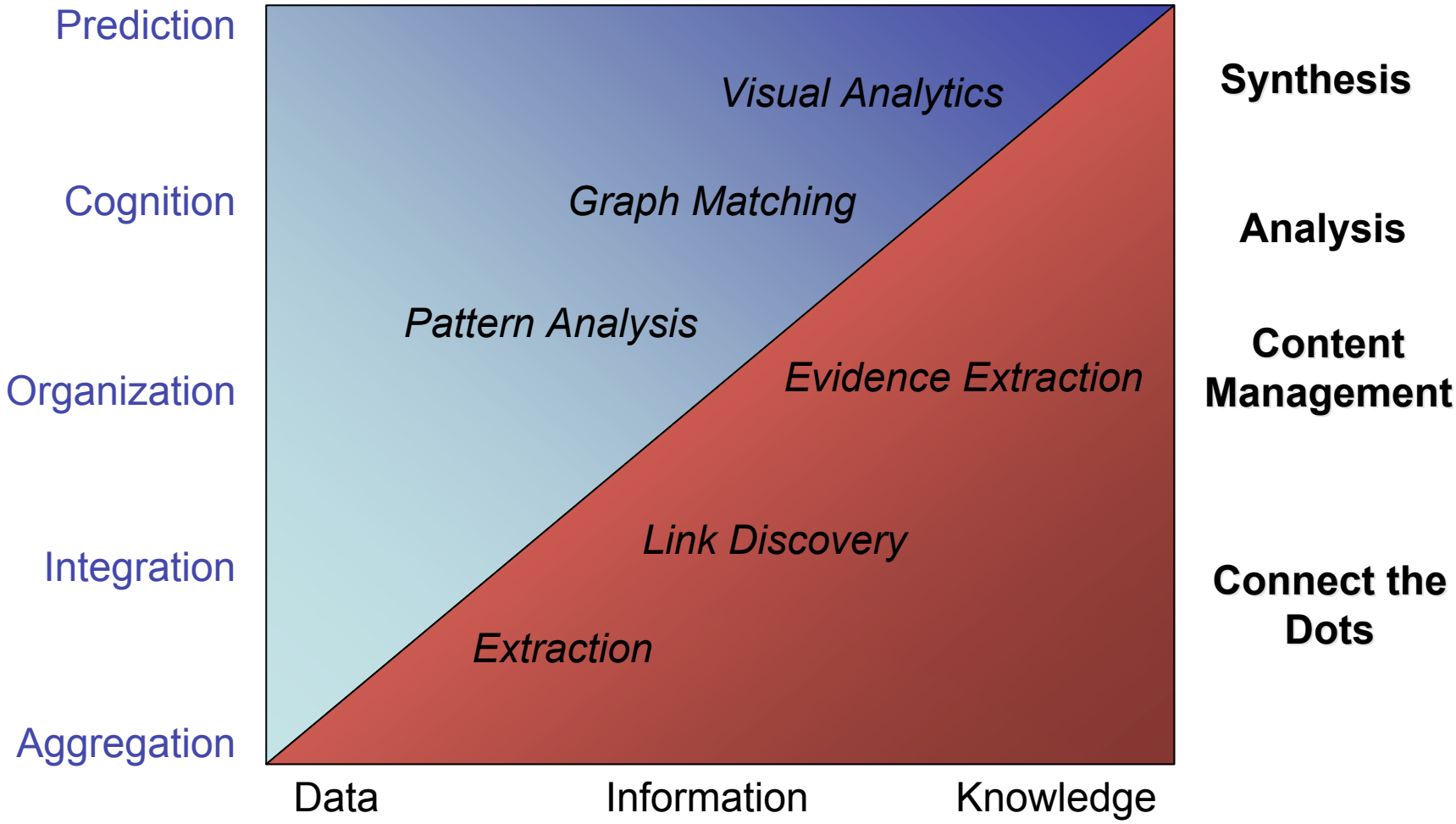
Evidence, not data, extraction is the goal

Complexity Level

IE Level	Type of Information Extracted			Status
	Entities	Relationships	Events	Technical
Deep Extraction ***Complex Semantics (Inferred Meaning)***		**Complex Semantic Relationships** • Merge information inferred to be on same event	**Deep Events (Scenarios) :** • Action (verb + sense) • Entities (plus roles) • All co-references • Ties to all related info • Time & Location	Beyond State-of-Art
Intermediate Extraction ***Basic Semantics (Meaning)***		**Simple Semantic Relationships, like** • Purchased-by • Employee-of	**Intermediate Events** • Action (verb + sense) • Entities (plus roles) • Simple co-references • Time & Location	State-of-Art
Shallow Extraction ***Syntax & Simple Patterns***	**Categories:** • People • Places • Organizations • Equipment • Quantities ($)	**Syntactic Relationships** Subject, verb, object... **Entities in same Events** **Entity Attributes, eg** • Gender, Ethnic Origin	**Shallow Events:** • Action (verb) • Entities (no roles) • Time & Location	Cots

Homeland Security

Multiple Techniques Contribute to Threat Assessment



Homeland Security

Analyzing Text Is Answering These Questions

- What does the text say?
- What does the text mean?
- How confident are we in that meaning?
- What more do we need to know?

Homeland Security

Homeland Security

Homeland Security